This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

Claim 1 (Currently amended): A session-state management method comprising:

generating an encoded session-state token, wherein the token incorporates a representation of session state of a client;

encrypting the encoded token ~~using a one-way encryption scheme~~ to produce an encrypted token that cannot be decrypted; and

sending the encrypted token to the client.

a18

Claim 2 (Original): A method as recited in claim 1, further comprising authenticating the user of the client.

Claim 3 (Original): A method as recited in claim 1, further comprising authenticating the user of the client, wherein the authenticating step comprises:

receiving a user identification indicator ("username") and a password;

comparing the username to a database of authorized user records, each record containing a username and a username-associated password;

comparing the password received in the receiving step to a username-associated password of a record containing a matching username; and

establishing a session for the user.

Claim 4 (Original): A method as recited in claim 1, wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block.

Claim 5 (Original): A method as recited in claim 1, wherein the generating step comprises forming a confirmation token that incorporates a representation of a current incremental time block.

Claim 6 (Original): A method as recited in claim 1, wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block that is prior a current incremental time block.

Claim 7 (Original): A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 1.

Claim 8 (Currently amended): A session-state management method comprising:

receiving an ~~one-way~~ encrypted, session-state token that cannot be decrypted from a client, wherein the token incorporates a representation of session state of a client;

generating an ~~one-way~~ encrypted, confirmation session-state token that cannot be decrypted; and

comparing the confirmation token with the received token.

Claim 9 (Original): A method as recited in claim 8, wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block.

Claim 10 (Original): A method as recited in claim 8, wherein the generating step comprises forming a confirmation token that incorporates a

representation of a current incremental time block.

Claim 11 (Original): A method as recited in claim 8, wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block that is prior a current incremental time block.

Claim 12 (Currently amended): A method as recited in claim 8, further comprising:

issuing an ~~one-way~~ encrypted, replacement session-state token that cannot be decryted; and

sending the replacement token to the client.

a18

Claim 13 (Original): A method as recited in claim 12, wherein the issuing step comprises forming a replacement token that incorporates a representation of a current incremental time block.

Claim 14 (Currently amended): A method as recited in claim 8, wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block, if confirmation and received tokens fail to match, the method further comprising:

generating a new ~~one-way~~ encrypted, confirmation session-state token that cannot be decrypted, wherein the confirmation token incorporates a representation of a previous incremental time block; and

comparing the new confirmation token with the received token.

Claim 15 (Currently amended): A session-state management method comprising:

receiving a one-way encrypted, session-state token from a client, wherein the token incorporates a representation of session state of a client;

generating a one-way encrypted, confirmation session-state token; and

comparing the confirmation token with the received token;

wherein the generating step comprises forming a confirmation token that incorporates a representation of an incremental time block, if confirmation and received tokens fail to match;

generating a new one-way encrypted, confirmation session-state token, wherein the confirmation token incorporates a representation of a previous incremental time block; and

comparing the new confirmation token with the received token;

~~A method as recited in claim 14,~~ wherein the new-confirmation-token generating step comprises forming a confirmation token that incorporates a representation of an incremental time block, if confirmation and received tokens fail to match~~, the method further comprising~~; and

repeating the steps of new-confirmation-token generating and comparing the new and received tokens, wherein each subsequent reiteration of such steps employs a representation of a previous incremental time block that is previous a previous reiteration of the same steps, for a specified number of times or until compared tokens match.

Claim 16 (Original): A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 8.

Claim 17 (Original): A session-state management method comprising:

(A) receiving a one-way encrypted, session-state token from a client;

(B) generating a one-way encrypted, confirmation session-state token, wherein the confirmation token incorporates a representation of a current incremental time block;

(C) comparing the confirmation token with the received token;

(D) if the confirmation token and the received token match,

(1) issuing a one-way encrypted, replacement session-state token, wherein the replacement token incorporates a representation of a current incremental time block;

(2) sending the replacement token to the client.

if the confirmation token and the received token fail to match,

(3) generating a new one-way encrypted, confirmation session-state token using the one-way encryption scheme of the encryption step, wherein the token incorporates a representation of a previous incremental time block;

(4) comparing the new confirmation token with the received token;

(5) if the new confirmation and received tokens fail to match, then further comprising:

(i) repeating the steps of new-confirmation-token generating and comparing the new and received tokens, wherein each subsequent reiteration of such steps employs a representation of a previous incremental time block that is previous a previous reiteration of the same steps, for a specified number of times;

(ii) if, during the repeating step, the confirmation token matches the

received token,

(a) issuing a one-way encrypted, replacement session-state token, wherein the token incorporates a representation of a current incremental time block;

(b) sending the replacement token to the client.

Claim 18 (Original): A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 17.

Claim 19 (Original): A session-state management method comprising:

authenticating a user of a client to establish a session with the user;

generating an encoded session-state token, wherein the encoded token incorporates a representation of session-state of the user's session;

encrypting the encoded token to produce an encrypted token that cannot be decrypted; and

sending the encrypted session-state token to the client.

Claim 20 (Original): A method as recited in claim 19, wherein the authenticating step comprises:

receiving a user identification indicator ("username") and a password;

comparing the username to a database of authorized user records, each record containing a username and a username-associated password;

comparing the password received in the receiving step to a username-associated password of a record containing a matching username; and

establishing a session for the user.

Claim 21 (Original): A method as recited in claim 19, wherein:

the user is identified by a user identification indicator (UserID);

the generating step comprises forming a session-state token at least partially based upon the UserID.

Claim 22 (Original): A method as recited in claim 19, wherein:

a time block is identified by a time block identification indicator (TimeID);

the generating step comprises forming a session-state token at least partially based upon the TimeID.

Claim 23 (Original): A method as recited in claim 19, wherein:

the user is identified by a user identification indicator (UserID);

a time block is identified by a time block identification indicator (TimeID);

the generating step comprises forming a session-state token at least partially based upon the UserID and the TimeID.

Claim 24-25 (Canceled)

Claim 26 (Original): A method as recited in claim 19, wherein:

the user is identified by a user identification indicator (UserID);

a time block is identified by a time block identification indicator (TimeID);

the generating step comprises combining UserID and TimeID to produce an encoded token.

Claim 27 (Original): A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 19.

Claim 28 (Currently amended): A session-state token generation method, wherein an authenticated user is identified by a user identification indicator (UserID) and a time block identification indicator (TimeID) identifies a specific time block, the method comprising:

combining UserID and TimeID to produce an encoded token;

encrypting the encoded token to produce an encrypted token that cannot be decrypted.

Claim 29 (Original): A method as recited in claim 28, wherein the combining step comprises concatenating UserID and TimeID.

Claim 30 (Original): A method as recited in claim 28, wherein the combining step comprises concatenating UserID, TimeID, and a code key.

a18

Claim 31 (Original): A method as recited in claim 28, wherein the encrypting steps comprises encrypting the encoded token using a one-way encryption scheme.

Claim 32 (Original): A method as recited in claim 28, wherein the encrypting steps comprises:

encrypting the encoded token using a one-way encryption scheme to produce an encrypted result; and

selecting a defined portion of the encrypted result to form a session-state token.

Claim 33 (Original): A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 28.

Claim 34 (Currently amended): A session-state management method comprising:

receiving a user-associated, encoded session-state token that cannot be decrypted from a client, wherein the encoded token incorporates a representation of session-state of the user's session;

generating an encoded, confirmation session-state token;

encrypting the encoded confirmation token to produce an encrypted token that cannot be decrypted; and

comparing the received token with the confirmation token.

Claim 35 (Original): A method as recited in claim 34, wherein the generating step comprises forming a confirmation token that incorporates a representation of a current incremental time block, if confirmation and received tokens fail to match, further comprising:

a 18

generating a new confirmation token using a representation of a incremental time block previous of the time block representation used for the previous generating step;

comparing the new confirmation token with the received token.

Claim 36 (Currently amended): A session-state management method comprising:

receiving a user-associated, encoded session-state token from a client, wherein the encoded token incorporates a representation of session-state of the user's session;

generating an encoded, confirmation session-state token;

comparing the received token with the confirmation token;

wherein the generating step comprises forming a confirmation token that

incorporates a representation of a current incremental time block, if confirmation and received tokens fail to match, further comprising:

generating a new confirmation token using a representation of a incremental time block previous of the time block representation used for the previous generating step;

comparing the new confirmation token with the received token; and

~~A method as recited in claim 35,~~ if confirmation and received tokens fail to match, ~~further comprising:~~and

repeating the steps of generating a new confirmation token and comparing the new and received tokens, wherein each subsequent reiteration of these steps uses a representation of a previous incremental time block that is ~~previous~~ a previous reiteration of the same steps, for a specified number of times or until compared tokens match.

a18

Claim 37-38 (Canceled)

Claim 39 (Original): A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method as recited in claim 34.

Claim 40 (Currently amended): A session-state management method comprising:

receiving an encoded token that cannot be decrypted comprising a user-associated TimeID from a client, wherein the encoded token incorporates a representation of session-state of the user's session;

designating a first time block identification indicator (TimeID) for a first time block; and

comparing the user-associated TimeID with the first TimeID.

Claim 41 (Currently amended): The method of claim 40, further comprising:

designating a prior TimeID for a time block prior to the first time block; and

comparing the user-associated TimeID with the prior TimeID.

Claim 42 (Currently amended): A server to communicate with a client over a communications network, the server comprising:

a processor; and

a session-state manager executable on the processor to:

generate a session-state token, wherein the token incorporates a representation of session state of the client;

encrypt the token ~~using a one-way encryption scheme~~ to produce an encrypted token that cannot be decrypted; and

send the encrypted token to the client.

Claim 43 (Currently amended): A server to communicate with a client over a communications network, the server comprising:

a processor; and

a session-state manager executable on the processor to:

receive an ~~one-way~~ encrypted, session-state token that cannot be decrypted from the client, wherein the token incorporates a representation of session state of a client;

generate an ~~one-way~~ encrypted, confirmation session-state token that cannot be decrypted; and

compare the confirmation token and the received token.

Claim 44 (Currently amended): A server to communicate with a client over a communications network, the server comprising:

a processor; and

a session-state manager executable on the processor to:

authenticate a user of the client;

generate an encoded session-state token, wherein the token incorporates a representation of session state of the client; ~~and~~

encrypt the session-state token into a token that cannot be decrypted; and

send the encrypted session-state token to the client.

Claim 45-46 (Canceled)

Claim 47 (Currently amended): A server to communicate with a client over a communications network, wherein an authenticated user is identified by a user identification indicator (UserID) and a time block identification indicator (TimeID) identifies a specific time block, the server comprising:

a processor; and

a session-state manager executable on the processor to:

combine UserID and TimeID to produce a encoded token; and

encrypt the encoded token into a token that cannot be decrypted.

Claim 48 (Currently amended): A server to communicate with a client over a communications network, the server comprising:

a processor; and

a session-state manager executable on the processor to:

receive a user-associated, encoded session-state token from the client;

generate an encoded, confirmation session-state token, wherein the confirmation token incorporates a representation of session state of the client;

encrypt the encoded token into a token that cannot be decrypted; and

compare the received token with the confirmation token.

Claim 49 (Currently amended): A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method comprising:

generating an encoded session-state token, wherein the token incorporates a representation of session state of a client;

encrypting the encoded token into a token that cannot be decrypted ~~using a one-way encryption scheme~~; and

sending the encrypted token to the client.

a18

Claim 50 (Currently amended): A computer-readable storage medium having computer-executable instructions that, when executed by a computer, performs the method comprising:

receiving an ~~one-way~~ encrypted, session-state token that cannot be decrypted from a client, wherein the token incorporates a representation of session state of a client;

generating an ~~one-way~~ encrypted, confirmation session-state token that cannot be decrypted; and

comparing the confirmation token with the received token.